

UNITED STATES DISTRICT COURT  
DISTRICT OF RHODE ISLAND

IN RE: SEARCH WARRANTS FOR :  
FIFTEEN CELLULAR TELEPHONES : Misc. No. 21-SW-164-PAS  
:

**AFFIDAVIT**

I, Rachel L. Robinson, Special Agent with the Department of Homeland Security, Homeland Security Investigations (“HSI”), having been duly sworn, depose and state as follows.

1. I am a Special Agent/Criminal Investigator with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”), and as a Special Agent of the United States Department of Homeland Security, I am authorized as an officer of the United States to conduct investigations and make arrests for offenses enumerated in Titles 8, 18, and 19 of the United States Code. I have been employed by HSI since May 2007. Prior to that assignment, I was employed as a Customs and Border Protection Officer with Customs and Border Protection for over four years. I am currently assigned to conduct investigations in the Resident Agent in Charge (RAC) Providence Office of HSI. I have prepared numerous affidavits in support of applications for federal search and arrest warrants. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

2. Based on my training and experience, I am familiar with the manner in which individuals involved in financial and document fraud use cellular telephones, media tablets, and other digital media devices to communicate with co-conspirators, create counterfeit documents, transfer stolen identity information and facilitate various aspects of their criminal activity.

3. I am submitting this affidavit in support of a search warrant to search the following items in furtherance of my investigation into violations of federal law, Conspiracy to Commit Access Device Fraud, 18 U.S.C. § 1029(b)(2), Access Device Fraud, 18 U.S.C. § 1029(a)(1), Possession of Access Device Fraud Equipment, 18 U.S.C. § 1029(a)(4), Aggravated Identity Theft, 18 U.S.C. § 1028A(a)(1) and Wire Fraud, 18 U.S.C. § 1343:

**Cellular phones seized by Warwick Police Department on July 03, 2020 following the arrest of Courtney HILAIRE, Shawn HILAIRE and Hugh MARTIN:**

- a. Black LG TracFone assigned Warwick Police property number 20-1411-PR-A;
- b. Black BLU TracFone bearing a NE Patriots sticker assigned Warwick Police property number 20-1411-PR-B;
- c. Black TCL TracFone assigned Warwick Police property number 20-1411-PR-C;
- d. Black TCL TracFone assigned Warwick Police property number 20-1411-PR-D;
- e. Black TCL TracFone assigned Warwick Police property number 20-1411-PR-E;
- f. Black TCL TracFone assigned Warwick Police property number 20-1411-PR-F;
- g. Black TCL TracFone IMEI: 015423002801071 seized from Courtney HILAIRE and assigned Warwick Police property number 20-1411-PR-G;
- h. Black LG TracFone assigned Warwick Police property number 20-1411-PR-H;
- i. Black TCL found rear right passenger side of the vehicle, assigned Warwick Police property number 20-1392-PR;
- j. Black TCL phone found in trunk, assigned Warwick Police property number 20-1401-PR;
- k. Black Alcatel TracFone assigned Warwick Police Department property number 20-1416-PR-A;

- l. Black TCL TracFone IMEI: 015423002809512 assigned Warwick Police property number 20-1416-PR-B;
- m. Black TCL TracFone IMEI: 015423008543388 assigned Warwick Police property number 20-1416-PR-C;
- n. Black TCL TracFone assigned Warwick Police property number 20-1416-PR-D;
- o. Black Alcatel TracFone assigned Warwick Police property number 20-1416-PR-E

4. The statements contained in this affidavit are based upon information from my personal observations and training and experience, and review of relevant records related to this investigation, as well as information provided to me by other local law enforcement officers and witnesses involved in this investigation.

**PROBABLE CAUSE**

5. On July 3, 2020, Courtney HILAIRE, as well as other conspirators were arrested by Warwick Police Department. Among the items recovered from the vehicle were mobile phones, credit cards in different identities, driver licenses from multiple states in different identities, a notebook containing handwritten entries of numerous identities and related personally identifiable information (PII) including address and dates of birth, a Lenovo Think Pad serial number R9-01MRTN 14/05 a black card cutter/mechanical press, a Staples Laminator 26530, MSR-X6 Magnetic Reader/Writer serial number 0171223223 an Apple Mac Pro computer serial number CO2CQ9TYMD6N an Epson XP-7100 scanner/printer serial number X5D5139942 and \$13,000 in U.S. currency.

6. The facts related to that incident were documented in an affidavit in support of federal search warrant for several mobile phones and computers. On July 21, 2020, the federal search

warrants were authorized by U.S. Magistrate Judge Patricia A. Sullivan issued warrants for those devices (*See generally* 20-SW-251, 20-SW-252, 20-SW-253 20-SW-254, 20-SW-255, 20-SW-256, 20-SW-257, and 20-SW-258). The affidavit in support of those warrants is true and correct to this day and is hereby incorporated by reference.

7. Pursuant to that warrant, qualified law enforcement personnel of HSI and the Warwick, Rhode Island Police, extracted electronic data from the devices seized incident to the Warwick arrest. On the Lenovo laptop computer investigators located electronic files identifying Courtney HILAIRE as the owner/primary user of the device. Special Agent David Riccio reviewed evidence extracted from the laptop. He noted that under the section of the extraction report titled “Chrome Top Sites” was the link <http://www.new-holos.com/>. This website offers holograms specific to United States driver’s licenses for sale that would be necessary to manufacture counterfeit driver’s licenses. Also listed under the section titled “Chrome Top Sites” was a bookmarked website with the link [https://mega.nz/#F!oKF3cjb!Fo\\_iTMLVwo7PCZrCZgZ1Vw](https://mega.nz/#F!oKF3cjb!Fo_iTMLVwo7PCZrCZgZ1Vw). This link leads to a webpage that displays a folder titled “FRAUD MEGAPACK” that is a 14.43 GB folder containing templates, fonts, unique characteristics and other images to create fraudulent driver’s licenses, credit cards, currency, birth certificates, diplomas, certificates and vehicle registrations. The folder is a virtual identity theft and counterfeiting kit. In addition to these two frequently visited sites under the “Chrome Top Sites” heading, was a site listed as a bookmarked website with the following link: <https://ssndob.cc/login>. This website provides personal identifying information for a fee. It is common for identity thieves to access the so-called “dark web” to purchase personally identifying information stolen during the illegal infiltration and theft of various databases to use to perpetrate their fraudulent schemes.

8. During Special Agent Riccio's review of the data the extracted from the Lenovo L440 laptop SN: R9-01MRTN 14/05 he noted it held ten fraudulent Maryland, North Carolina and Washington driver's licenses. He caused queries to be conducted on each of the licenses and determined the information displayed on the fraudulent licenses matched information on file for real people. He noted that two of the fraudulent licenses contained digital photographs of COURTNEY HILAIRE and HUGH MARTIN.


9. On August 6, 2020, HILAIRE was arrested by Pawtucket Police Department in the area of 49 Darrow Street. Incident to that arrest, Pawtucket Police Officer Barrett seized \$2,399.00 cash from HILAIRE. In HILAIRE's pocket Officer Barrett seized Visa cards, two of them with the name Courtney HILAIRE and others bearing the names David Z. Petty, Irian Tolchin, John Gralton, Brian Leclair, Peter T. Keith and Gail Frisch. Pawtucket Police also seized an Apple iPhone Rose Gold and 2 LG Metro color black incident to HILAIRE's arrest.


10. On August 13, 2020, a federal search warrant was authorized by U.S. Magistrate Judge Patricia A. Sullivan for the Apple iPhone Rose Gold seized from HILAIRE on the day of his arrest by Pawtucket Police Department, (*See generally* 20-SW-287-PAS, 20-SW-288, and 20-289.) The affidavit in support of those warrants is true and correct to this day, is also incorporated by reference.

11. Pursuant to a search warrant, authorized personnel conducted a data extraction from the Apple iPhone Rose Gold seized from HILAIRE by the Pawtucket Police. I have reviewed the data extracted from this device. There are numerous files including photograph, Telegram message "chats," video images and notes that evidence the device was owned by and regularly used by Courtney HILAIRE.


12. Based upon my training and experience, my conversations with other members of law enforcement and my review of literature involving identity theft, I am aware that identity thieves often communicate using cellular telephone devices including the type seized by the Warwick Police and Pawtucket Police. I am further aware that there have been recent cases of identity theft and bank fraud here in the District of Rhode Island where members of an identity theft fraud ring, used their cellular devices to exchange personal identifying information, photographs for use in creating counterfeit government identifications and business locations with security vulnerabilities. More importantly, as set out in the following paragraphs, I am aware the Apple iPhone Rose, seized by the Pawtucket Police contained a plethora of electronic evidence demonstrating a consistent pattern and reliance upon electronic devices identical to the device I currently am seeking authorization to search.

13. Pursuant to the warrant issued for the Apple iPhone Rose, representatives of U.S. Homeland Security Investigations conducted a data extraction of the Apple iPhone Rose Gold. I have reviewed some of that evidence and have personally observed a tremendous amount of evidence that HILAIRE has been involved in multiple Identity Fraud and Financial Fraud schemes including Unemployment Insurance claims from multiple states and Small Business Administration (SBA) loans which have been offered as a result of the COVID-19 pandemic. The iPhone also contained chats providing detailed instructions and advice related to how to commit SBA fraud and secure funds from SBA without detection. One specific chat was with HILAIRE and an individual using the name James Dominguez. In this chat, HILAIRE gives specific instructions on how to commit SBA fraud detailing 20 different steps on how to complete the transaction. The iPhone also contained numerous sets of stolen personal identifiable information (PII) used to perpetrate these frauds. Hilaire relied heavily on these

devices to commit these crimes. There were videos located on the phone in which an individual documented the preparation and submission of loan applications using stolen identities. There was also a video of HILARE holding a large amount of cash and kissing it. In the notes section, contained PII of numerous victims of state unemployment insurance fraud. The following is a snapshot of chat messages from HILAIRE (MrVACATION) in the telegram chat entitled “Trap School (FF) ”<sup>1</sup>

- a.) 7/23/20 (4:04 pm) Video scrolling through an email titled Deposit returned “Hi Courtney, a deposit of \$9500.00 from SBAD TREAS 310 was returned to the depository. We are only able to accept direct deposits where the receiver’s name on the deposit matches the name of the Chime account holder. To correct this deposit please contact the depositer who initiated this transaction. Sincerely, the Chime Team.”<sup>2</sup>
- b.) 7/29/20 (4:31 am) message sent stating “100k day” followed by a video showing numerous cell phones near a computer.
- c.) 7/29/20 (9:31pm) video displaying a screen shot of numerous SBA loan application approvals with a green check mark over them bearding the label “MrVacation.”
- d.) 7/31/20 (11:05am) message stating “My bitches just ran up 80k easy !!!” followed by a video of four females sitting in a living room.
- e.) 8/1/20 (2:09 pm) Video sent to “Trap School (FF) ” stating “TM LOVE” conducting an ATM withdrawal of a large sum of money.
- f.) 8/2/20 (11:06 am) Chat messages stating “another batch!! Ya niggas know I work for real..SBA PAYOUT THIS TUESDAY. Don’t miss it. We going uppppp (several surf,

---

<sup>1</sup> By my personal knowledge and by reviewing the chat titled “Trap School (FF) ,” trap school is a reference to teaching others how to deceive unsuspecting victims and run a scam.

<sup>2</sup> Chime is an online internet based financial service that offers a Visa debit card and a spending account that is managed from a smartphone, plus an optional savings account.

fire and check mark emojis) send In all cash apps n Chimes.” This message contained a video of numerous debit cards, to include US Bank Visa, lined up with a giant green check mark over them bearing the label “MrVacation.”

g.) 8/3/20 (11:40 am) – Video of a very large amount cash what appears to be all 20 dollar denominations. Hilaire states he had a card that just “let me pull out 2200 out the TM. No Cap.” Hilaire then shows a withdrawal receipt from Citizens Bank, 478 Broadway, Central Falls RI, date 8/3/20 at 11:21 am with the card number ending in 7128. Hilaire states “see that last 4? 7128?” He then displays another Citizen Bank withdrawal receipt at Citizens Bank, 478 Broadway, Central Falls RI, date 8/3/20 at 11:22 am with the card number ending in 7128; stating “another one, no cap.” Hilaire then displays another Citizen Bank withdrawal receipt at Citizens Bank, 478 Broadway, Central Falls RI, date 8/3/20 at 11:20 am with the card number ending in 7128 and states “another one.” Hilaire then displays another Citizen Bank withdrawal receipt at Citizens Bank, 478 Broadway, Central Falls RI, date 8/3/20 at 11:19 am with the card number ending in 7128 and Hilaire states “see that’s \$1600 already off one piece.”

h.) 8/3/20 (12:41 pm) “Pullup 7k out of the atm today and it’s not even 1pm.”

i.) 8/3/20 (1:20 pm) A video of HILAIRE displaying large amounts of cash in rubber bands saying “two days ago” and displaying brand new Dior sneakers and a receipt for Sack Fifth Avenue in the amount of 2151.04 on 8/1/2020.

j.) 8/3/20 (1:32pm) A video where HILAIRE is speaking and showing various US Bank Debit cards, where what appears to be a lottery ticket covering the names on the cards. The last 4 or 6 numbers of the cards are visible and they appear to be US Bank Debit



cards seized by Pawtucket Police from the trash pull conducted on August 14, 2020 at 49 Darrow Street, Pawtucket, Rhode Island.

14. On August 6, 2020, during the arrest of Hilaire, Pawtucket Police Department seized a US Bank card ending in 7128, bearing the name, John Gralton. Gralton has since been interviewed and is a confirmed victim of this scheme.

15. On March 5, 2021, your affiant served a Grand Jury Subpoena to US Bank. On March 16, 2021, a response was received with the transaction history for card ending in 7128, bearing the name of a known victim John Gralton, confirms these withdrawal receipts on the video.

16. On March 7, 2021, at approximately 0216 hours, Officers of the Cranston Police Department responded to the Edgewood Laundry located at 1980 Broad St, Cranston, RI 02905 for a motor vehicle accident. Responding Officers located a black Dodge Charger bearing FL Registration CIKJ17 with severe damage to the front bumper and found that it had struck the Edgewood Laundry. That vehicle is registered to Enterprise Holdings Inc. The operator of that vehicle was identified as Courtney HILAIRE (DOB: XX/XX/1992), and the passengers were identified as Vladimir FONTAINE (DOB: XX/XX/1993) and Oliver FONTAINE (DOB: XX/XX/1995).

17. As a result of the Cranston Police Department's investigation, HILAIRE was charged with DUI/DRUGS/ALCOHOL/1ST OFFENSE - B.A.C. UNKNOWN in violation of RIGL 31-27-2-D1/M and REFUSAL TO SUBMIT CHEMICAL TEST in violation of RIGL 31-27-2.1.

18. Officers further reported that when conducting a motor vehicle inventory search of the vehicle, a large amount of U.S. currency was located on the front driver's side floor where

HILAIRE was previously sitting. Officers also located a large amount of U.S. currency inside the center console that was wrapped in a \$100 band. Officers later conducted a count of the U.S. currency and found it to be a total of \$7,168.00 (CPD Property # 21-637-PR). Officers also reported that HILAIRE was in possession of an Apple iPhone cell phone (CPD Property # 21-636-PR) TARGET DEVICE. HILAIRE's cell phone and the U.S. currency were later transported to the Cranston Police Department where it was entered into evidence to be held for safe keeping.

19. Each interaction with law enforcement, HILAIRE has possessed a large amount of U.S. Currency and he also possessed cellular device(s). Those cellular device(s) contained a tremendous evidence of the aforementioned fraud schemes.

20. On March 15, 2021, HSI Providence seized a Blue Apple iPhone belonging to Courtney HILAIRE, that was being held at Cranston Police Department following HILAIRE's arrest by Cranston Police on March 7, 2021. On March 19, 2020, a federal search warrant was authorized by U.S. Magistrate Judge Patricia A. Sullivan for the Blue Apple iPhone seized from HILAIRE (2021\_SW-113-PAS).

21. On April 2, 2021, the grand jury in the District of Rhode Island, returned an indictment charging Courtney HILAIRE, Shawn HILAIRE and Hugh MARTIN, with a variety of federal offenses including, Conspiracy to Commit Access Device Fraud, 18 U.S.C. § 11029(b)(2), Access Device Fraud, 18 U.S.C. § 1029(a)(1), Possession of Access Device Fraud Equipment 18 U.S.C., § (a)(4), Aggravated Identity Theft. Incident to the return of the indictment his Court issued an arrest warrant for Courtney HILAIRE.

22. As a result of Courtney HILAIRE's arrest by the Cranston Police, the State of Rhode Island moved to revoke HILAIRE's bail. The state District Court initially ordered

Courtney HILAIRE ordered detained. The Court subsequently ordered HILAIRE transferred from the Intake Service Center and placed him into Community Confinement to be served at 15 Piedmont Street second floor apartment Providence, RI.

23. On April 5, 2021, your affiant, accompanied by other members of HSI and the Providence Police, responded to 15 Piedmont Street second floor apartment to execute the arrest warrant. At approximately 7:45 a.m. the Rhode Island Department of Corrections called HILAIRE and instructed him to open the door to his apartment for investigators. HILAIRE opened the door and agents entered. Your affiant was aware that HILAIRE was sharing the apartment with others and due to the early hour concluded there were possibly other occupants present who could interfere with the arrest. During a protective sweep of the apartment I observed a large stack of United States currency located on a bathroom vanity. In the bedroom where HILAIRE had been sleeping and had his clothes, I observed a large stack of cash on the nightstand. I observed a second sealed package on the nightstand that had the shape and weight consistent with another package of cash. I also observed what appeared five cellular telephones and two laptop computers, an Apple and a Samsung laying on the bed. One of five cellular devices was later identified as a Moxee Mobile Hotspot. On the floor immediately next to the bed, I observed a cash counting machine. In the kitchen area, I observed a credit card swiping machine used to read and embedded magnetic stripes with data. On the couch in the living room area, I observed an additional cellular telephone.

24. As a result, a search warrant was authorized by U.S. Magistrate Judge Patricia A. Sullivan for 15 Piedmont St, Unit 2, Providence RI 02909 (2021-SW-140-PAS). As a result of the search warrant, HSI Providence seized \$47,119.00 in cash, eleven (11) mobile devices (3 of which still in original packaging), a Moxee mobile hotspot device, Apple Watch Series 5, Apple

MacBook Pro laptop computer, Samsung Chromebook laptop computer, Cassida Currency Counter, Deftun Card reader, value cards and bank cards, and miscellaneous documents.

25. Pursuant to that search warrant, authorized personnel conducted a data extraction from the mobile devices seized from HILAIRE. I have reviewed data extracted from the ZTE mobile device that was found in the kitchen drawer. Under the section Web History, I observed the following: Rhode Island Unemployment Insurance website; Pennsylvania's Pandemic Unemployment Assistance Portal (within that portal, history of Registration, My Dashboard, Applying for Unemployment Insurance, Unemployment Insurance Claim Status, Claim Certification, Insurance Claim Confirmation, Employment History Review, Customer Satisfaction Survey, Benefits Plan Profile, Weekly Certifications Review List); Online services for Individual (<https://Applications.labor.ny.gov/Individual>); Unemployment Insurance Claimant Information (<https://Applications.labor.ny.gov/Individual>); NY.gov ID Login; ROBOCHECK USA SSNDOB-History; Key2Benefits Unemployment Card Status KeyBank; US Bank reliacard/card-order status-tracker; Employment Development Department (<https://uio.edd.ca.gov>); Log in to Online Services (<http://edd.ca.gov/login.htm>); NC Division of Employment Security::New Account Registration.

26. Also on the same ZTE mobile device, under the section Searched Items, I observed Searched Items to include "pa pua lo," "pa pua login;" "ca pua login;" "bank of america edd;" "keybank check status;" "nc pua login;" "ny pua login."

27. Based on my experience and training, my conversations with other members of law enforcement and my review of literature involving identity theft, I am aware that the presence of the credit card embosser, the printer, laptop computers and the laminating machine recovered by the Warwick Police on July 3, 2020, all support the conclusion that C. HILAIRE,

S. HILAIRE and H. MARTIN were actively involved in the creation of counterfeit credit cards and identifications. The subsequent discovery of additional counterfeit credit cards and government identifications by the Pawtucket Police incident to the arrest of COURTNEY HILAIRE on August 6, 2020, the amount of cash in HILAIRE'S possession on the night of the Cranston Police incident on March 7, 2021, as well as the amount of cash in HILAIRE'S possession on at the time of his federal arrest on April 05, 2021, leads me to conclude that despite law enforcement action in July 2020, August 2020, March 2021, and April 2021, COURTNEY HILAIRE and others have remained involved in committing offenses of access device fraud and conspiracy to do the same. My conclusion is further supported by observations made by TFO Matthew Smith concerning postings made to Courtney HILAIRE's Facebook social media account "Prince Hill". These postings include a post on January 14, 2021 that states "50 flights in a Year!! Blow 20k every trip (two palm tree emojis) living better than your favorite rapper". A post was made on December 25, 2020 that states "Puerto Rico (flag emoji) Tomorrow everything paid for (four exclamation point emojis) Bad bitches hit my line". The Facebook profile picture for "Prince Hill" was updated on November 13, 2020 which shows an image of Courtney HILAIRE with the text "Atm Runs" at the bottom of the image. These posts support additional evidence that HILAIRE is living a lavish lifestyle with no legitimate source of income. Further, I have reason to believe that electronic evidence related to the creation of counterfeit credit cards and identification documents needed to further perpetrate credit card fraud is likely to be found on the TARGET DEVICES.

28. By examining the previously referenced electronic devices, it has become apparent to me that the cellular telephones S. HILAIRE, C. HILAIRE and H. MARTIN possessed in July 2020 will contain additional electronic evidence linking them to a larger

number of incidents of wire fraud. I say this because I am now aware that individuals carrying out fraudulent schemes targeting the SBA and state unemployment systems have discovered that those programs have firewalls or tripwires that look for common telephone numbers associated with benefit applications. Accordingly, perpetrators will employ multiple prepaid cellular telephones to carry out their scheme. I am also aware that it is reasonably likely trained personnel will be able to, at the very least, extract the phone number the device had last been assigned. Using that information, your affiant and other members of the investigative team can obtain additional process directing the respective state unemployment systems previously identified on C. HILIARE's devices as well as the SBA to search for applications associated with those telephone numbers.

### **SEARCH OF ELECTRONIC DEVICES**

28. Based upon my experience and training I know that electronic devices like the TARGET DEVICES can store information for long periods of time. This information includes photographs, word processing documents, emails and other types of documents and records containing information needed to carry out identity theft, access device fraud and bank fraud.<sup>3</sup> Similarly, things that have been viewed via the internet are typically stored for some period of time on the devices.<sup>4</sup> This information can sometimes be recovered with forensics tools.

29. As further described in Attachment B, this application seeks

---

“Records, documents, and materials,” as used herein, includes all information recorded in any form by any means, whether in handmade form (such as writings, drawings, or paintings), photographic form (such as developed film, print-outs, slides, negatives, or magazines), type-written form (such as print-outs, books, pamphlets, or other typed documents), audio/visual form (such as tape-recordings, videotapes, DVDs, or CDs), or electronic form (such as digital data files, file properties, computer logs, or computer settings)

<sup>4</sup> “Internet,” as used herein, refers to a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.


permission to locate electronically stored information as well as forensic evidence that establishes how the TARGET DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET DEVICES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a cellular telephone is evidence may depend on other information stored on the cellular telephone and the application of knowledge about how a cellular telephone behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit the examination of the TARGET DEVICES consistent with the warrants which may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrants.

31. Based on the foregoing, there is probable cause to believe that THE TARGET DEVICES, seized from Courtney HILIARE, Shawn HILAIRE and Hugh MARTIN by the Warwick Police on or about July 03, 2020, contain personally identifiable information (PII) for victims of identity fraud, images of counterfeit drivers licenses and other identity documents, communications between parties involved in identity fraud and access device fraud, and other data that constitutes evidence of the above listed offenses.

  
RACHEL L. ROBINSON  
Special Agent

Rachel L. Robinson  
Special Agent, Department of Homeland Security

Attested to by the applicant in accordance with the requirements of Fed.  
R. Crim. P. 4.1 by \_\_\_\_\_.  
(specify reliable electronic means)

Date

Judge's signature

City and State

Printed name and title



**ATTACHMENT B**  
**ITEMS TO BE SEIZED**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely Conspiracy to Commit Access Device Fraud, 18 U.S.C. § 1029(b)(2), Access Device Fraud, 18 U.S.C. § 1029(a)(1), Possession of Access Device Fraud Equipment 18 U.S.C., § (a)(4), Aggravated Identity Theft, and Wire Fraud 18 U.S.C. § 1343.

- a. Records and information relating to the telephone number the TARGET DEVICE had last been assigned.
- b. Records and information related to the collection and transfer of personal identification information (PII) including Social Security Numbers, dates of birth, home addresses, driver's license numbers, credit card account numbers, places of employment and educational history;
- c. Records and information relating to the creation of counterfeit and fraudulent government identification including driver's license templates, hologram and authentication features, corporate logos for financial institutions and credit card companies using PII;
- d. Records and information relating to applications for lines of credit and access to financial institution accounts using stolen PII to include savings, checking, money market and investment accounts;
- e. Records and information relating to the transfer of money including crypto currency utilizing any application or money transfer software and the actual transfer of money and any record documenting the transfer and location of money;
- f. Records and information relating to email accounts including emails discussing the commission of the within named federal offenses;
- g. Records and information relating to the identity or location of the suspects;
- h. Records and information relating to communications with Internet Protocol addresses.
- i. evidence of who used, owned, or controlled the COMPUTER/TARGET DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- j. evidence of software that would allow others to control the COMPUTER/TARGET DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- k. evidence of the lack of such malicious software;
- l. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- m. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- n. evidence of the attachment to the COMPUTER/TARGET DEVICE of other storage devices or similar containers for electronic evidence;
- o. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER/TARGET DEVICE;
- p. evidence of the times the COMPUTER/TARGET DEVICE was used;
- q. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER/TARGET DEVICE;
- r. documentation and manuals that may be necessary to access the COMPUTER/TARGET DEVICE or to conduct a forensic examination of the COMPUTER/TARGET DEVICE;
- s. records of or information about Internet Protocol addresses used by the COMPUTER/TARGET DEVICE ;
- t. records of or information about the COMPUTER/TARGET DEVICE’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- u. contextual information necessary to understand the evidence described in this attachment.